संख्या-8/2026/ए-1-34/आई/1343278/2026-10-31/18/2026

प्रेषक,

दीपक कुमार,
अपर मुख्य सचिव,
उत्तर प्रदेश शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उत्तर प्रदेश शासन।

वित्त (लेखा) अनुभाग-1 लखनऊ : दिनांक 27 मई, 2026

विषय : ई-प्रोक्योरमेंट प्रणाली की प्रभावशीलता और परिपक्वता के मूल्यांकन हेतु निष्पादित की गयी लेखापरीक्षा के प्रबन्धन पत्र के सम्बन्ध में।

महोदय,

कृपया उपर्युक्त विषयक कार्यालय महालेखाकार (लेखापरीक्षा-प्रथम) ऑडिट भवन, 15-ए, दयानन्द मार्ग, उत्तर प्रदेश, प्रयागराज के पत्र संख्या-प्र0म0ले0(लेखापरीक्षा-I)/आई.एण्डपी0एफ0/फ0सं013/2023-24/67, दिनांक 30.04.2026 व उसके साथ संलग्न भारत के नियंत्रक एवं महालेखापरीक्षक के प्रबन्धन पत्र (छायाप्रति संलग्न) का अवलोकन करने का कष्ट करें।

2- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि कृपया उक्त सन्दर्भित पत्र में की गयी अपेक्षानुसार अपने स्तर से आवश्यक कार्यवाही करने का कष्ट करें।

संलग्नक : यथोपरि।

भवदीय,

दीपक कुमार
अपर मुख्य सचिव।

संख्या एवं दिनांक तदैव।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1- कार्यालय महालेखाकार (लेखापरीक्षा-प्रथम) ऑडिट भवन, 15-ए, दयानन्द मार्ग, उत्तर प्रदेश, प्रयागराज-211001
2- अपर मुख्य सचिव/प्रमुख सचिव/सचिव, श्री राज्यपाल, उत्तर प्रदेश।
3- प्रमुख सचिव/विधान सभा/विधान परिषद, उत्तर प्रदेश।

आज्ञा से,

महेन्द्र कुमार भट्ट
विशेष सचिव।

http://shasanadesh.up.gov.in

1- यह शासनादेश इलेक्ट्रानिकली जारी किया गया है, अत: इस पर हस्ताक्षर की आवश्यकता नहीं है।
2- इस शासनादेश की प्रमाणिकता वेब साइट https://shasanadesh.up.gov.in से सत्यापित की जा सकती है।

सं०-ई-34/दस-2026

कार्यालय प्रधान महालेखाकार
(लेखापरीक्षा-प्रथम)
ऑडिट भवन, 15-ए, दयानन्द मार्ग,
उत्तर प्रदेश, प्रयागराज-211001

OFFICE OF THE
PRINCIPAL ACCOUNTANT GENERAL
(AUDIT-I)
Audit Bhawan, 15-A, Dayanand Marg,
Uttar Pradesh, Prayagraj -211001

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

पत्रांक: प्र०म०ले०(लेखापरीक्षा-I)/आई.एण्ड पी.ए./ फ.सं.13 /2023-24/67
दिनांक 30-04-2026

सेवा में,

प्रमुख सचिव,
वित्त विभाग,
उत्तर प्रदेश शासन,
लखनऊ-226001

विषय- ई-प्रोक्योरमेंट प्रणाली की प्रभावशीलता और परिपक्वता के मूल्यांकन हेतु निष्पादित की गयी लेखापरीक्षा के प्रबन्धन पत्र के संबंध में।

महोदय,

भारत के नियंत्रक एवं महालेखापरीक्षक द्वारा ई-प्रोक्योरमेंट की प्रभावशीलता और परिपक्वता का मूल्यांकन करने के लिए देश के 12 राज्यों में सूचना प्रणाली (IS) लेखापरीक्षा सम्पादित की गयी थी।

इस सम्बन्ध में अवगत कराना है कि लेखापरीक्षा के निष्कर्षों के आधार पर उत्तम प्रथाओं का उल्लेख, प्रणालीगत कमियों की पहचान तथा उनके निराकरण हेतु सुझाव को समाहित करते हुए एक प्रबंधन पत्र (Management Letter) तैयार किया गया है तथा विभागीय स्तर से आवश्यक कार्यवाही किये जाने हेतु प्रेषित किया जा रहा है।

कार्यालय सं० 4998 /अ०मु०स०वि०/दस-सा०/2026 दिनांक: 12/05/26

यह पत्र प्रधान महालेखाकार महोदय के अनुमोदन से प्रेषित किया जा रहा है।

भवदीय

उपमहालेखाकार
ए०एम०जी०-III

संलग्नक-यथोपरि

11/05/26
(दीपक कुमार)
अपर मुख्य सचिव
वित्त एवं वित्त आयुक्त, संस्थागत वित्त
एवं वाह्य सहायतित परियोजना विभाग
उत्तर प्रदेश शासन।

पत्रांक: प्र०म०ले०(लेखापरीक्षा-I)/आई.एण्ड पी.ए./ फ.सं.13 /2023-24

प्रतिलिपि:

1. प्रमुख सचिव, सूचना प्रोद्योगिकी एवं इलेक्ट्रॉनिक्स विभाग, उत्तर प्रदेश शासन, लखनऊ को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।
2. प्रमुख सचिव, नगर विकास विभाग, उत्तर प्रदेश शासन, लखनऊ को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

वित्त (लो०प०) अनु

14.5.2026
(आलोक दीक्षित)
विशेष सचिव
वित्त (लो०प०) विभाग
उत्तर प्रदेश शासन

उपमहालेखाकार
ए०एम०जी०-III

Phone: 0532-2420447 Fax: 0532-2424102 E-mail:agauuttarpradesh1@cag.gov.in

श्री सर्वजीत
15.05.2026

COMPTROLLER AND AUDITOR GENERAL OF INDIA

MANAGEMENT LETTER

Information Systems Audit of

e-Procurement System across States

March 2026

New Delhi

TABLE OF CONTENTS

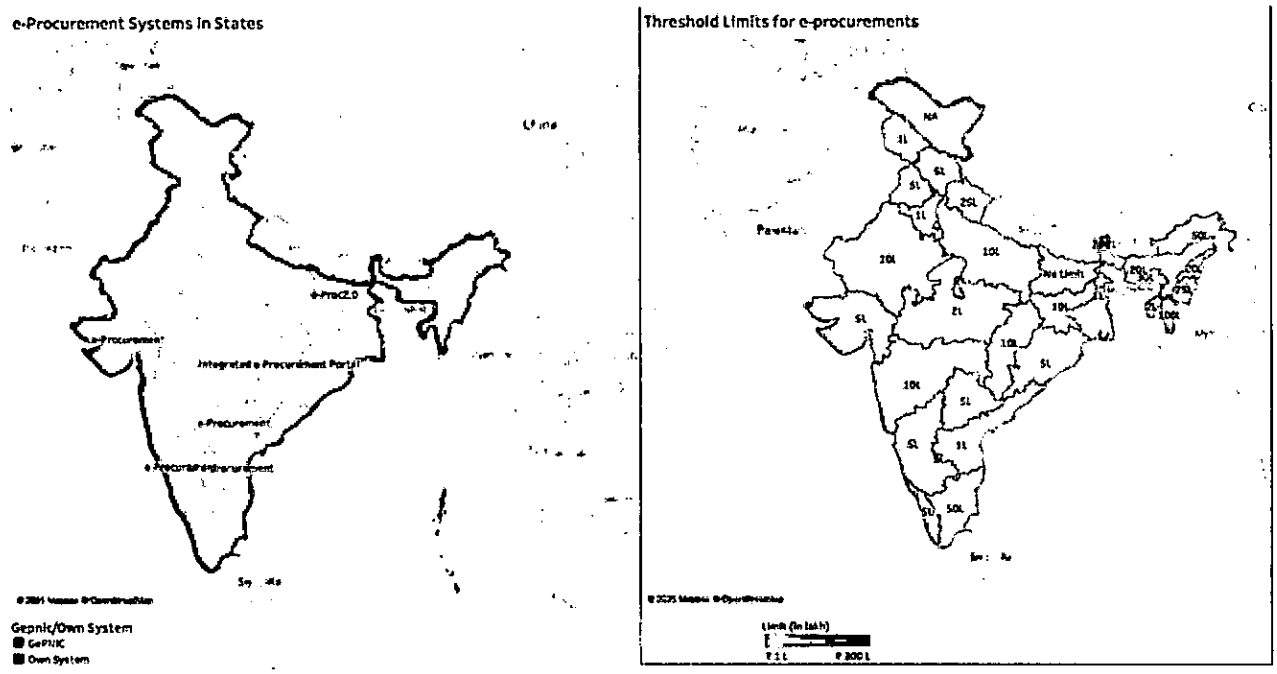
Section	Particulars	Page No.
I	Introduction: Background, Objectives, Criteria, Scope and Methodology	3
II	Areas of Progress in the States on use of e-Procurement systems	6
III	Analysis of Common Causal Relationships across States	8
IV	Summary of Audit Findings across the States	10
V	Recommendations	22
	Annexure-I: Status of IS Audit Reports on e-Procurement Systems in the States	24
	Glossary of Abbreviations	25

1. Introduction

1.1 Background and Context

Electronic Procurement (e-Procurement) refers to the use of Information and Communication Technology (ICT) by Government entities to procure goods, works and services through electronic platforms. Under the National e-Governance Plan (NeGP), the Government of India introduced e-Procurement as a Mission Mode Project, and the National Informatics Centre (NIC) developed the Government e-Procurement System (GePNIC) for adoption by States. As on February 2026, States and the Central Government have published 1.64 crore tenders valuing ₹246.22 lakh crore since inception (2011), with 4.50 crore bids received through NIC's system.

In the States, e-procurement is mandated for procurements above thresholds ranging from ₹1 lakh to ₹50 lakh. In addition to e-tendering, many States have adopted the Government e-Marketplace (GeM) portal for procurement of goods and services, promoting transparency, competition, and cost-effectiveness.



e- Procurement systems and threshold limits for e-procurement in the States

1.2 Audit of e-Procurement Systems

Over the last decade, most State Governments have adopted GePNIC or State-customised e-Procurement portals to enhance transparency and fairness in procurement, ensure non-discrimination among bidders, promote competition and value for money, reduce procurement cycle time, strengthen accountability and audit trails, and integrate procurement systems with financial management systems such as IFMS/IFMIS.

The Comptroller and Auditor General of India has conducted Information Systems (IS) Audit of the Implementation of e-Procurement System in 12 States. IS Audit Reports in respect of Assam, Odisha, Punjab and Tamil Nadu have been tabled in the State Legislative assemblies. IS Audit reports for the States of West Bengal, Himachal Pradesh, GNCT of Delhi and Uttar Pradesh have been shared with the

respective State Governments and are yet to be tabled in the State legislative assembly. In the State of Andhra Pradesh and Telangana, management letter has been issued to the State Government on the important audit outcome emanating from the IS audit of the e-procurement systems in the State. The reports of Haryana and Jharkhand are under the process of approval for sharing with the State Legislature. This Management Letter consolidates audit objectives, findings, systemic issues and recommendations emerging from these State audits into common thematic observations. The status of all 12 e-Procurement IS Audit Reports is given at Annexure-I.

1.3 Audit Objectives

Audit assessed whether the e-Procurement system of the State Governments operates as a secure, integrated and end-to-end digital procurement platform that ensures compliance with the applicable regulatory framework, embeds procurement business rules and application controls, maintains data integrity and system security, and promotes transparency, accessibility, non-discriminatory bidder participation, competition, effective oversight and accountability in procurement activities.

1.4 Audit Criteria and Scope

The audit criteria were derived from the General Financial Rules (GFR 2017), respective State Financial Rules, Public Works Codes, Transparency in Public Procurement Acts and Rules, CVC guidelines on e-tendering, and World Bank procurement guidelines. In addition, audits were benchmarked against the IT Act 2000, STQC guidelines for e-Procurement systems, NIC implementation guidelines for GePNIC, Software Requirement Specifications, Service Level Agreements, Master Service Agreements, and ISO 27001 standards.

The scope generally covered the period from 2018-19 to 2022-23 and examined the end-to-end workflow of e-Procurement systems, covering the Registration Module, Tender Publishing Module, Bid Submission Module, Tender Opening and Evaluation stages, Award of Contract module, and system security features including audit logs, encryption standards, Disaster Recovery (DR) mechanisms, data migration and database integrity controls.

1.5 Audit Methodology

The audits adopted a combination of qualitative and quantitative approaches. Entry and Exit Conferences were held with nodal departments. Extensive use was made of Computer Assisted Audit Techniques (CAATs) including IDEA, PostgreSQL, SQL-based queries, Tableau and Excel analytics for large-scale data analysis. Database dumps of e-Procurement portals were analysed to identify anomalies in tender lifecycle tracking, IP address mapping, EMD transaction patterns, bidder participation trends and award decisions. Field audits were conducted in selected departments and districts using risk-based sampling, with review of project documentation, system design artefacts, SLA compliance records and governance frameworks.

1.6 Rationale for this Common Management Letter

Audits were conducted independently across States, where recurring systemic deficiencies were observed despite adoption of common technological platforms. These deficiencies included partial implementation of modules, inadequate mapping of financial rules, absence of critical validation controls, weak

monitoring mechanisms, lack of automated red flag systems, incomplete IFMS integration, deficiencies in log management, and insufficient enforcement of governance frameworks.

The persistence of similar issues across the States indicates structural and design-level challenges rather than isolated operational lapses. This consolidated Management Letter presents theme-wise findings across States, identifies common causal factors and proposes structured recommendations to strengthen governance, improve control frameworks, enhance system integrity, and embed real-time analytics.

II. Areas of Progress and Unique Initiatives in the States on use of e-Procurement systems

Several notable achievements in the implementation of e-Procurement across States were observed during the Audit. These areas of progress form an important foundation for further reform.

State	Unique Initiative
Andhra Pradesh	• Adoption of GePNIC as a common State-wide platform; coverage of large procurement volumes through a single portal; integration of online payment for Earnest Money Deposit (EMD) and tender fees; availability of historical procurement data for data analytics. • The State has a dedicated State e-Procurement portal with separate e-Tender and e-Auction domains; mandatory e-Auction for disposal of scrap and surplus assets.
Assam	• Adoption across 45 of 56 Departments; 26,855 tenders worth ₹1,19,849.31 crore (2018-22) processed, integration of online payment mechanisms; centralised procurement data is available. • Integration of e-Procurement within the broader AS-CFMS/ASPIRe public financial management reform framework under single nodal coordination by the Finance Department.
GNCT of Delhi	• A total of 1,54,586 tenders valuing ₹1,01,098.67 crore were published through e-procurement system during the period 2017-23 (upto May 2023). • State-wide adoption of a common e-Procurement platform; centralised tender publication and bidder registration; availability of system-generated MIS and historical data for data analytics.
Haryana	• Adoption across 162 organisations; 2.46 lakh tenders worth ₹2.12 lakh crore processed (2018–23). • State-wide adoption of GePNIC; introduction of online payment for tender fees and EMD; centralised tender information for public access; identification of high-value items for GeM routing.
Himachal Pradesh	• Roll-out across multiple Departments with electronic bid submission; basic role-based access with Digital Signature Certificate (DSC) mapping; Management Information System (MIS) reports on tender activity; reduced reliance on physical documentation.
Jharkhand	• State-wide platform adoption with electronic publication and bid submission; basic role-based access controls configured; electronic records maintained; standard MIS reports available. Initial rollout in 9 Departments, later intended for all Departments (phased expansion)
Odisha	• Adoption across 29 of 40 Departments; 3,74,806 tenders worth ₹3,31,908 crore processed; STQC certification obtained.

	• Development of Contractor Database Management System (CDMS) Phase-I for centralised registration and validation of contractors; Integration attempt with WAMIS for works management alignment; online lottery functionality for transparent selection.
Punjab	• Adoption across 45 Departments / 2,111 procurement entities; 1,85,920 tenders processed (2018–23). • Punjab Transparency in Public Procurement Act, 2019 and Rules, 2022 enacted as a statutory framework; NIC primary and DR site at National Data Centres.
Tamil Nadu	• Early GePNIC adoption since 2008; online bid submission with encryption and DSC authentication; SBI integration for online EMD collection. • Development of new portal from April 2023 incorporating audit recommendations; plans for centralised online vendor registration with Unique IDs; digital M-Book and common schedule of rates under development.
Telangana	• State-wide e-Procurement portal and e-Auction system established; online bid submission and publication; online payment for EMD and transaction fees; centralised data for analytics. • Customised e-Procurement portal under State-specific Master Service Agreement; centralised oversight through Telangana Technology Services Limited (TGTS); consolidation of procurement-related funds for system sustenance.
Uttar Pradesh	• During the period 2018-23, tenders for 10.31 lakh work items costing ₹ 9.34 lakh crore were invited in the State through GePNIC system in which total 26.72 lakh bids were submitted by the participating bidders. • State-wide GePNIC availability; high procurement volumes processed; MeitY security/transparency certification during audit period; MIS reports capturing bidder IP addresses and participation patterns.
West Bengal	• Mandatory e-Procurement above ₹50 lakh since 2012, progressively reduced to ₹1 lakh ensuring widest possible bidder access; 9.75 lakh tenders worth ₹5.23 lakh crore processed; 52 of 54 Departments using portal. • SMS/email notifications to bidders improved communication; online bid opening with DSC.

III. Analysis of Common Causal Relationships across States

Audit identified the following five recurring causal factors underlying the systemic deficiencies across all 12 States, despite differences in State-specific contexts:

A. Governance and Accountability Deficits

The most pervasive causal factor across all States was the absence of a formal governance framework for e-Procurement. No State had executed comprehensive MoU/SLA arrangements with NIC or other service providers, creating ambiguity in roles, timelines, deliverables and escalation mechanisms. Project Steering Committees and Monitoring Units were either not constituted, inactive, or inadequately staffed. Absence of a designated 'Centre of Responsibility' to coordinate portal issues, enforce compliance and drive corrective action was a universal gap. Periodic performance reviews, post-implementation audits, and structured change management were not institutionalised in any State.

B. Inadequate Mapping of Procurement Rules into System Logic

The e-Procurement systems in all 12 States failed to comprehensively translate statutory procurement rules and executive instructions into automated application controls. Minimum bid submission periods under GFR 2017 and State Financial Rules were not system-enforced. Two-bid processes for large-value tenders, delegated financial powers, validity periods, eligibility criteria and EMD computation rules were not mapped into system workflows. This created scope for manual discretion at critical decision points, undermining the fundamental objective of rule-based, non-discriminatory procurement.

C. Over-reliance on Manual Processes and Offline Controls

Technical evaluation, financial bid assessment, negotiation with L1 bidders, award of contracts, and EMD management continued to be processed offline in most States despite the existence of an e-Procurement platform. This persistence of manual controls alongside electronic systems created multiple points of vulnerability for manipulation, reduced the reliability of audit trails, and undermined end-to-end process integrity. In several States, the e-Procurement system functioned effectively only as a tender publication and bid receipt portal, with all critical decision-making remaining outside the system.

D. Weak Validation and Application Controls

Application-level validation controls were inadequate across all stages of the procurement lifecycle in all 12 States. Systems accepted invalid and duplicate bidder credentials, tenders with incomplete mandatory fields, zero-value estimated contract values, invalid dates and inconsistent data. Role segregation, maker-checker controls and access management were poorly configured. Blocked or deactivated users retained system access in several States. These design-level deficiencies enabled participation by ineligible bidders, duplicate registrations, and potential for manipulation of tender records.

E. Absence of Analytics, Exception Monitoring and Red-Flag Detection

None of the 12 States had deployed real-time analytics, automated red-flag dashboards or exception monitoring tools within the e-Procurement system. Despite large volumes of transactional data being available, the data was not harnessed for supervisory oversight, competition monitoring or collusion detection. Patterns of bid rotation, common IP usage, shared credentials and sequential EMD instruments

that were identifiable through data analytics went undetected by the systems themselves. Reliable MIS reports for management decision-making were absent or underutilised in all States.

IV. Summary of Audit Findings across the States

The following section presents the audit findings State-wise, organised across seven thematic dimensions- digitisation, transparency, efficiency, project implementation, control weakness, security and compliance, and collusion and competition.

1. Andhra Pradesh

The State achieved extensive digitisation of tender publication, bidder registration, bid submission and fee collection across departments. However, certain deficiencies and gaps were observed by Audit which are listed below:

i. Critical procurement lifecycle components such as automated bid evaluation, contract award, contract management and catalogue management were not implemented, digitisation remained largely confined to front-end activities, with key decision-making stages continuing to be handled manually outside the system.

ii. Absence of system-enforced rules, incomplete updating of tender status, offline negotiations and physical issuance of Letters of Award weakened transparency of bid evaluation and award processes. Audit trails for approvals, deviations and post-bid modifications were not comprehensively captured in the system.

iii. Non-enforcement of minimum bid submission periods, lack of automated validations and delays in updating tender status adversely impacted efficiency. Significant pendency of tenders at intermediate stages indicated limited managerial oversight through the system.

iv. Procurement rules were not comprehensively translated into system logic, and changes in executive instructions were not promptly reflected in application controls.

v. Audit identified pervasive application control deficiencies across bidder registration, tender publication, bid submission, bid evaluation and award of contracts. The system permitted manual determination of bid timelines, EMD and transaction fees, participation of ineligible contractors, offline bid evaluation and negotiations, and processing of tenders beyond delegated financial powers. These weaknesses increased reliance on administrative discretion and undermined uniform enforcement of procurement rules.

vi. Validation controls, segregation of duties and exception monitoring were inadequate, although the system was operational for a prolonged period. Incomplete data validation, weak master-data controls and lack of structured MIS dashboards limited assurance over data integrity and compliance.

vii. Large-scale data analysis revealed significant incidence of bids submitted using common IP addresses, mobile numbers and email IDs, including use of Departmental IP addresses for bid submission. Absence of automated alerts, analytical dashboards and preventive controls constrained the system's ability to detect or deter collusive bidding and cartelisation.

Some illustrations:

a. Delegation of financial powers bypassed: Tender Inviting Authorities (TIAs) published and awarded hundreds of tenders whose values far exceeded their delegated financial powers without obtaining competent authority approval, due to the absence of application controls linking user roles to financial limits.

b. Vulnerabilities in bidder master data: The system allowed bidders to modify their master data (e.g., class certificates) during active bid submission rather than requiring a separate, verified master data update, creating a massive risk of fraudulent qualification.

2. Assam

Assam implemented GePNIC for procurement of goods, works and services and processed a substantial volume of tenders through the portal. However certain deficiencies and gaps were observed by Audit which are listed below:

i. Incomplete on-boarding of all departments and organisations, coupled with continued reliance on offline processes for bid evaluation and contract award, resulted in only partial digitisation of the procurement lifecycle. The declining trend in the number of tenders processed through the portal further indicated limited institutional adoption.

ii. Inadequate uploading of mandatory documents, delayed updating of tender status, and non-generation of system-based Awards of Contract during electronic submission of tender notices and bid submissions, reduced transparency of procurement outcomes. A large number of tenders remained shown as 'in progress' or 'to be opened' for extended periods, even where procurement had been concluded offline, thereby undermining the credibility of public disclosures and MIS.

iii. Audit observed prolonged delays between bid opening and award of contracts, with several tenders taking multiple years to reach closure. Absence of system-enforced timelines, automatic cancellation mechanisms and stage-wise monitoring significantly constrained efficiency gains.

iv. There was no effective system of periodic review to ensure that departments complied with prescribed workflows, timelines and data-updating requirements.

v. Significant application control deficiencies were observed across bidder registration, tender processing and award stages. These included lack of validation for mandatory bidder data, absence of system checks for minimum bid submission periods, acceptance of tenders with less than the prescribed number of technically qualified bidders, and weak controls over tender cancellation and re-tendering. The system permitted manual workarounds, increasing dependence on administrative discretion.

vi. Key security and integrity concerns persisted, Although the system was certified by STQC including weak linkage of Digital Signature Certificates with registered users, absence of unique identifiers for mobile numbers and email IDs, missing audit logs for certain users, and unexplained gaps in database records. These deficiencies reduced assurance regarding data integrity, non-repudiation and accountability.

vii. The system lacked built-in analytical tools and preventive controls. Insufficient validation of bidder identities and credentials, combined with weak monitoring of participation patterns, limited the ability of the platform to deter collusive bidding or cartelisation.

Some illustrations:

a. Bidders allowed without digital signatures: 42.38% of users were registered without a Digital Signature Certificate (DSC), and 12,273 users actively participated in bidding without a DSC, nullifying the legal authenticity of the bids.

b. Complete lack of authentication controls: The system possessed no validation to match the name of the DSC holder against the registered application user. Consequently, multiple distinct DSCs were mapped to single User IDs, allowing unauthorized individuals to impersonate legitimate bidders.

3. GNCT of Delhi

The introduction of GePNIC in Delhi enabled online publication of tenders and electronic bid submission in a majority of cases. However, certain gaps were observed by audit which are listed below:

i. Critical stages such as EMD submission, technical evaluation and award of contract continued to be processed offline or manually, limiting end-to-end digitisation.

ii. Manual evaluation, offline EMD handling, incomplete audit trails and non-updating of award of contract details diluted transparency and limited public oversight.

iii. Efficiency gains were constrained due to short bid submission periods, manual interventions and incomplete workflow integration. Average competition levels did not show commensurate improvement.

iv. Implementation suffered from incomplete configuration of modules, inconsistent compliance by Tender Inviting Authorities (TIAs) and inadequate monitoring by the nodal department, resulting in partial achievement of project objectives.

v. Significant control weaknesses were observed in user registration, input validation, business rule mapping, bid evaluation sequencing and enforcement of procurement norms, exposing the system to risks of manipulation.

vi. Weak validation of PAN, email IDs, mobile numbers and Digital Signature Certificates (DSCs), and absence of controls over superannuated users, compromised system security and regulatory compliance.

vii. Multiple indicators of suspected collusion were observed, including use of common PANs, email IDs, mobile numbers and IP addresses by bidders and departmental users within the same tenders, undermining fair competition.

Some illustrations:

a. Conflict of interest: Bidders submitted 14,527 valid bids using the same IP addresses used by departmental users during the tendering process, indicating suspected collusion and compromised bid secrecy.

b. System access by superannuated staff: There were no access controls to prevent retired departmental users from logging in; some even participated in opening and evaluating bids post-superannuation.

4. Haryana

Haryana implemented the e-Procurement system across departments and published a large volume of tenders through the GePNIC platform. Core stages such as tender publication, bid submission and electronic payment of fees were operationalised. However, certain gaps were observed by audit which are listed below:

i. Critical modules such as indent management, contract management and catalogue management were not implemented, resulting in continued reliance on offline processes for key procurement activities. Consequently, digitisation remained partial and transactional, rather than process-centric.

ii. Transparency objectives were weakened due to non-updation of tender stages, incorrect award details, non-uploading of evaluation summaries and absence of tamper-proof audit trails. A substantial number of tenders remained in 'published' or intermediate stages for extended periods, limiting public and managerial oversight.

iii. Absence of system-enforced timelines, weak validations, manual bid evaluation and lack of reliable MIS reports constrained efficiency gains. Inadequate training of users and under-resourced project monitoring arrangements further reduced effective utilisation of system functionalities.

iv. Although the system was operational for over a decade, formal governance mechanisms were weak. No agreement was executed with NIC, the Project Monitoring Unit (PMU) was inadequately staffed, and periodic performance reviews were not institutionalised. Post-implementation enhancements, corrective actions on earlier audit observations and structured change management were not effectively carried out.

v. Significant control deficiencies were observed across the tender lifecycle, including user registration, segregation of duties, tender scheduling, corrigenda issuance, bid opening sequence, evaluation and award of contracts. The system permitted manual overrides and post-deadline interventions, increasing dependence on administrative controls and weakening assurance over fairness and consistency.

vi. Audit noted the absence of documented change management, business continuity and disaster recovery plans. Weak access controls, missing or incomplete logs and inadequate alert mechanisms reduced assurance regarding data integrity, non-repudiation and compliance with prescribed procurement rules.

vii. Limitations in system analytics, validation controls and automated alerts significantly constrained e-Procurement platform's ability to detect or deter collusive practices. Recurrent patterns such as bids from the same IP address, identical credentials, sequential EMD instruments and post-deadline bid extensions indicated vulnerabilities that undermined fair competition.

Some illustrations:

a. Financial loss due to missing controls: The system lacked controls to retain non-refundable tender document and e-service fees. This design flaw resulted in the erroneous refund of ₹19.71 crore to bidders.

b. Collusive bidding: 68,390 bids were submitted from the exact IP addresses used by government departmental users. The system failed to generate alerts for multiple bids originating from common IPs, mobile numbers, and PANs.

5. Himachal Pradesh

The adoption of electronic procurement resulted in increased digitisation of procurement processes, particularly in relation to tender publication, bid submission and maintenance of electronic records. The transition from manual to electronic processes reduced dependence on physical documentation and enabled wider dissemination of tender information. However, certain gaps were observed by audit which are listed below:

i. Deficiencies in system-driven controls, audit trail mechanisms and supervisory oversight limited the extent to which transparency objectives were fully realised, particularly at critical stages of the tender lifecycle.

ii. Transparency objectives were weakened due to non-updation of tender stages, incorrect award details, non-uploading of evaluation summaries and absence of tamper-proof audit trails. A substantial number of tenders remained in 'published' or intermediate stages for extended periods, limiting public and managerial oversight.

iii. Absence of system-enforced timelines, weak validations, manual bid evaluation and lack of reliable MIS reports constrained efficiency gains. Inadequate training of users and under-resourced project monitoring arrangements further reduced effective utilisation of system functionalities.

iv. Although the system was operational for over a decade, formal governance mechanisms were weak. No agreement was executed with NIC, the Project Monitoring Unit (PMU) was inadequately staffed, and periodic performance reviews were not institutionalised. Post-implementation enhancements, corrective actions on earlier audit observations and structured change management were not effectively carried out.

v. Significant control deficiencies were observed across the tender lifecycle, including user registration, segregation of duties, tender scheduling, corrigenda issuance, bid opening sequence, evaluation and award of contracts. The system permitted manual overrides and post-deadline interventions, increasing dependence on administrative controls and weakening assurance over fairness and consistency.

vi. Audit noted the absence of documented change management, business continuity and disaster recovery plans. Weak access controls, missing or incomplete logs and inadequate alert mechanisms reduced assurance regarding data integrity, non-repudiation and compliance with prescribed procurement rules.

vii. Limitations in system analytics, validation controls and automated alerts significantly constrained e-Procurement platform's ability to detect or deter collusive practices. Recurrent patterns such as bids from the same IP address, identical credentials, sequential EMD instruments and post-deadline bid extensions indicated vulnerabilities that undermined fair competition.

Some illustrations:

a. Financial loss due to missing controls: The system lacked controls to retain non-refundable tender document and e-service fees. This design flaw resulted in the erroneous refund of ₹19.71 crore to bidders.

b. Collusive bidding: 68,390 bids were submitted from the exact IP addresses used by government departmental users. The system failed to generate alerts for multiple bids originating from common IPs, mobile numbers, and PANs.

5. Himachal Pradesh

The adoption of electronic procurement resulted in increased digitisation of procurement processes, particularly in relation to tender publication, bid submission and maintenance of electronic records. The transition from manual to electronic processes reduced dependence on physical documentation and enabled wider dissemination of tender information. However, certain gaps were observed by audit which are listed below:

i. Deficiencies in system-driven controls, audit trail mechanisms and supervisory oversight limited the extent to which transparency objectives were fully realised, particularly at critical stages of the tender lifecycle.

ii. Absence of robust system validations and limited use of MIS and exception reports constrained the realisation of optimal efficiency gains.

iii. Periodic system reviews and structured performance assessments were not adequately institutionalised, affecting long-term sustainability.

iv. The audit identified control weaknesses in user access management, segregation of duties, tender lifecycle controls, bid security management, audit trail maintenance and monitoring arrangements. Periodic review of user accounts was not carried out, inactive user IDs remained enabled, and maker-checker controls for critical activities were not consistently enforced. System validations governing tender modification, corrigenda, bid submission timelines and bid opening were insufficient, allowing scope for manual intervention at sensitive stages. These weaknesses reduced reliance on system-embedded controls and increased dependence on manual supervision.

v. The absence of comprehensive tamper-proof audit logs, inadequate input and processing controls and absence of access reviews undermined assurance regarding data integrity, non-repudiation and compliance with prescribed procurement procedures.

vi. Limitations in analytics, monitoring tools and exception reporting reduced the system's ability to detect patterns indicative of restrictive competition or collusive behaviour, thereby constraining the full competitive potential of e-Procurement.

Some illustrations:

a. Tender splitting: High-value contracts were deliberately split into smaller jobs (sub-threshold) by departments to avoid e-tendering, resulting in a lack of competition and award of works at highly inflated prices (up to 156% above estimated costs).

b. Compromised procurement integrity: Bids were repeatedly submitted from the IP addresses of the procuring entities themselves, strongly indicating bid rigging and internal collusion.

6. Jharkhand

The e-Procurement system was implemented in Jharkhand for electronic publication of tenders and online submission of bids. However, certain gaps were observed by audit which are listed below:

i. Several critical stages of the procurement lifecycle such as bid evaluation and award of contracts continued to rely on offline or manual processes, limiting end-to-end digitisation.

ii. Incomplete audit trails, inadequate system logs and delayed or non-updating of tender stages reduced transparency at key decision points.

iii. Electronic tendering reduced procedural delays at the publication stage. However, manual interventions, weak system validations and limited use of MIS reports constrained the efficiency gains expected from e-Procurement.

iv. Monitoring mechanisms and post-implementation reviews were not institutionalised, affecting consistent and effective utilisation of the platform.

v. Audit identified significant control weaknesses in user access management, segregation of duties, tender lifecycle controls, bid security management and supervisory oversight. Periodic review of user accounts was not undertaken, inactive user IDs remained enabled and segregation of duties was inadequate. System

validations for tender modification, corrigenda issuance, bid submission timelines and bid opening were weak, allowing scope for manual intervention. Controls relating to tracking, adjustment and timely refund of bid securities were inadequate and audit trails were incomplete. These deficiencies led to increased dependence on manual supervision.

vi. Deficiencies in audit trail maintenance and periodic access reviews undermined assurance regarding data integrity, non-repudiation and compliance with prescribed procurement procedures.

vii. The absence of advanced analytics, exception reporting and competition-monitoring tools limited the system's ability to detect patterns indicative of restrictive competition or cartelisation, thereby constraining the effectiveness of e-Procurement as a tool for promoting fair competition.

Some Illustrations:

a) Audit discovered evidence of collusive bidding. A cartel of five interrelated firms (sharing staff, tools, and familial ties) manipulated water supply tenders finalized at ₹719.29 crore using dummy bids, subletting, and rotational L1 bidding. Overall, 131 cases of rotational bidding patterns were identified where the same pairs of bidders took turns becoming L1, often submitting bids from the same IP addresses within minutes of each other.

b) Conflict of interest (shared IPs & DSCs): Bids were repeatedly submitted from the exact static IP addresses explicitly allocated to the procuring departments (e.g., Forest Department), proving that bidders used departmental computers. Astonishingly, audit also found an instance where a departmental user and a participating bidder were using DSCs mapped to the same Computer Operator.

7. Odisha

Odisha adopted the NIC-developed GePNIC system in 2008, covering modules for tender publishing, bid submission and award of contracts. Major departments — Works, Rural Development and Water Resources — adopted the portal widely. However, certain gaps were observed by audit which are listed below:

i. Smaller departments and local bodies lagged behind, with several continuing to issue tenders manually. Without a State-wide mandate, adoption remained incomplete. While major departments migrated to the portal, many smaller entities continued manual procurement, limiting full digitisation.

ii. While tenders are published online, critical transparency gaps persist. Tender evaluation reports and contract awards were not consistently uploaded, forcing reliance on manual records. Several tenders were processed offline after initial online publication, preventing complete visibility in the portal. Inadequate public disclosure of award data reduced opportunities for citizen oversight, and non-publication of award details combined with incomplete audit trails and manual interventions reduced visibility for stakeholders.

iii. Although digitisation was expected to reduce procurement cycle time, efficiency remained mixed. Delays in award of contract were noted, with tenders pending finalisation far beyond prescribed timelines. EMD refunds to unsuccessful bidders were delayed due to continued reliance on offline modes. Some departments reverted to manual processing of negotiations or tie-breaks, slowing tender completion. Bid timelines under Odisha General Financial Rules were not enforced automatically, and the system allowed tenders with incomplete or incorrect data due to weak segregation of roles and inadequate input validation.

iv. The eProcurement project lacked robust governance. The Project Steering Committee and the eProcurement Cell did not meet regularly to review performance. There was no clear 'Centre of Responsibility' to enforce compliance or resolve systemic issues. Capacity building was limited — training for department officials was irregular and vendor outreach was minimal, reducing bidder participation and effective use of the portal.

v. Audit highlighted multiple control deficiencies. Key rules from Odisha's procurement framework were not incorporated into the system, including strict bid submission timelines and automatic enforcement of validity periods. Tenders were accepted with missing mandatory fields or incorrect data entries such as null values and incorrect classifications. Multiple nodal officers were created in some entities, while blocked or deactivated users could still access parts of the system. Tender processing sometimes bypassed system controls, reducing the reliability of audit trails.

vi. Security measures were inadequate. Disaster recovery drills were infrequent and not all departments had contingency arrangements. No evidence of periodic security audits or penetration testing was available. Audit logs were not consistently maintained, leaving the system vulnerable to unauthorised access. Provisions for negotiation and purchase preference policies were not encoded in the system. Analysis of audit trails revealed backend manipulation of 72 tenders.

vii. The system did not prevent collusive practices. Some tenders received bids from the same set of vendors repeatedly, with patterns suggesting bid rotation. In several cases, only one or two bids were received, limiting competition. Without analytics or monitoring, such anti-competitive practices went undetected.

Some illustrations:

a. Database integrity and security breaches: There were gaps in system-generated sequential IDs in critical database tables (e.g., over 2.56 lakh missing records in the gep_bids table) alongside missing web and application logs. This points to unauthorized manual deletion/modification of bid data at the backend.

b. Invalid decryption of bids: Financial bids were irregularly decrypted without any record of the technical bids being decrypted. Moreover, symmetric keys of bids were decrypted by users *other than* the designated bid openers.

8. Punjab

Major departments use the portal, but smaller agencies often continued parallel manual procurement or hybrid processes. Certain gaps were observed by audit which are listed below:

i. Full digitisation of the procurement lifecycle — particularly bid evaluation, negotiations and contract award — was not achieved.

ii. Non-publication of evaluation reports and award details reduced visibility, undermining the transparency objectives of the portal.

iii. Offline handling of negotiations, delays in EMD refunds and weak enforcement of tender timelines limited efficiency gains. 52,046 out of 1,85,920 published tenders — 28 per cent — were cancelled over five years, indicating poor tender planning and an overall portal success ratio of only 59 per cent.

iv. The nodal department had not executed a MoU with NIC to ensure legal sanctity, accountability and clarity of roles, despite assurances given by NIC and PAC recommendations. Similarly, no MoU was in place with the SBI payment gateway. The Project Steering Committee met irregularly, vendor training was limited and monitoring of usage was ineffective. Non-preparation of annual procurement plans by procuring entities was also observed.

v. The system lacked robust input validation and business-rule mapping, allowing tenders with null or incorrect values, duplicate user roles and incomplete data. Irregularities in offline technical and financial bid evaluation were noticed in 122 of 494 sample tenders. Offline collection of EMD was observed in 46 tenders, in contravention of prescribed rules. Absence of blacklisting functionality and delays in enforcing debarments were noted. Discrepancies were noticed in bid decryption dates for the same packet, and in the use of Digital Signature Certificates.

vi. Security audits were delayed, disaster recovery arrangements were untested and audit trails were incomplete. In 3,389 out of 44,081 instances, IP location was not captured by the system; in 49 instances, the IP location was outside India.

vii. Audit analysis indicated repeated participation of the same bidders, limited competition and bid-rotation patterns. Multiple registered users were found with common email IDs, mobile numbers and PAN numbers, and bidders with common credentials participated in the same tenders.

Some illustrations:

a. Collusion via PAWAN network: Bids were submitted using the Punjab State Wide Area Network (PAWAN) IP addresses explicitly allocated to the procuring departments. This confirms that bidders utilized departmental systems to place bids, completely compromising bid secrecy.

b. System malfunctions forcing date extensions: System failures on NIC's end forced the automatic extension of bid submission dates for 2,896 tenders without any request from the procuring authorities, leading to overlapping opening and submission dates.

9. Tamil Nadu

The GePNIC platform was implemented in 2008 and offers eight modules covering registration, publishing, bid submission, opening, evaluation and award of contract. By 2022, about 2.97 lakh tenders valued at ₹2.92 lakh crore had been published. However, certain deficiencies and gaps were observed by audit which are listed below:

i. Adoption remained partial. Out of 201 procuring entities, 148 never used the portal. Even among users, only 12 per cent of tenders reached the award-of-contract stage online, the rest being diverted to manual processes.

ii. Transparency, a key objective, was diluted. Tender stages were not updated and summary reports for evaluation and award were often missing. Tamil Nadu ranked 11th among 15 GePNIC-using States in terms of updating contract awards online. Tender evaluation continued manually in many cases despite provisions for online submission. Non-upload of evaluation reports perpetuated dependence on offline records and reduced visibility for the public.

iii. Efficiency goals were not fully realised. Online EMD functionality was introduced in 2017, yet 73 per cent of tenders collected EMD offline, causing refund delays and diversion of ₹16.93 crore of EMD funds for administrative expenses. Processing delays were widespread: in 5,726 tenders, award of contract took longer than the validity period, with delays extending up to 1,552 days. Prescribed timelines under TNTIT Rules were not enforced in the software.

iv. No 'Centre of Responsibility' existed to coordinate portal issues or enforce compliance. Training and vendor awareness was minimal, covering only six per cent of registered officials and leaving bidders under-informed. A planned centralised vendor registration workflow was not executed, limiting bidder participation and competition.

v. Minimum bid submission periods and domestic purchase preferences were not incorporated as business rules. Tenders with zero values, null entries in mandatory fields and duplicate PANs were common. Multiple nodal officers per entity, role conflicts and blocked users participating in or updating tender records were identified. Process failures included bids being decrypted on different dates and buy-back tenders with miscalculated comparative charts.

vi. Security audits by STQC were outdated, with several software versions deployed after certification without re-audit. Public access to tender documents was restricted beyond the download period, limiting transparency. Compliance with TNTIT Rules was weak. Provisions for negotiation, tie-breaking and purchase preference were missing in the software. Evaluation of tenders sometimes relied on inconsistent criteria, ignoring GST or ISO compliance.

vii. Audit analysis released multiple patterns of anti-competitive behaviour. Sixty two per cent of tenders had only one or two bids. Contracts were rotated between fixed bidder pairs in TNCSC and DRDA tenders. Relatives submitted parallel bids in 35 tenders.

Some illustrations:

a. Cartelisation & bid rigging: Audit discovered evidence of collusive bidding. Competing bidders systematically submitted bids from the same IP addresses (sometimes from within the procuring entity's own office). Bidders also uploaded offline EMD Demand Drafts with *consecutive serial numbers* bought from the same bank branch on the same day.

b. Coded bidding communication: Uploaded EMD files were explicitly named with codes like 'L1', 'original', 'L2', or 'dummy' by the bidders, proving that the winning and losing bids were pre-determined through collusion.

10. Telangana

Telangana implemented a new e-Procurement portal covering e-Tendering and e-Auction modules, replacing the earlier system. However, certain gaps were observed by audit which are listed below:

i. Inordinate delays in development and rollout, coupled with non-migration of legacy data, resulted in fragmentation of procurement records and limited continuity of digital information. Several stages of procurement, including contract award and work order issuance, continued to be processed outside the system, resulting in partial digitisation of the procurement lifecycle.

ii. Deficiencies in input validation, incomplete data capture and non-updating of tender status undermined transparency, although tenders were published and bids submitted electronically. Publication of tenders without valid administrative and technical sanctions, zero estimated contract values and prolonged non-finalisation of tenders reduced the reliability of information available in the public domain.

iii. The objective of improving procurement efficiency through automation was not fully achieved. Audit observed prolonged delays between bid submission and award of contracts, extensive manual evaluation of bids and lack of system-enforced timelines. Absence of automated bid evaluation tools and vendor profiling increased manual workload for Tender Inviting Authorities and contributed to inefficiencies.

iv. Implementation of the e-Procurement project suffered from significant delays vis-à-vis contractual timelines stipulated in the Master Service Agreement. Several stipulated modules and functionalities remained undeveloped or partially implemented. Post-implementation governance, contract management and performance monitoring mechanisms were weak, particularly in respect of operation and maintenance arrangements.

v. Audit identified systemic application control deficiencies across bidder registration, tender publication, bid evaluation and fund management. Weak validation controls allowed submission of incomplete or incorrect bidder data, participation of ineligible contractors, multiple registrations and acceptance of tenders in violation of prescribed rules. Manual overrides and offline controls diluted the effectiveness of system-based safeguards.

vi. Key security and integrity controls were inadequate, including weak linkage of digital identities, absence of complete audit trails and gaps in tender ID sequencing. Compliance with procurement rules depended largely on manual verification rather than automated enforcement through the application.

vii. The portal lacked effective analytical and preventive controls to detect or deter collusive bidding. Audit observed multiple bidders using identical PANs, bank accounts, contact details and IP addresses, as well as instances where bids were submitted from the same IP addresses used by TIAs. These deficiencies significantly weakened assurance regarding fair competition and conflict-free procurement.

Some illustrations:

a. Bypassing maximum premium rules: The system lacked functionality to enforce the maximum ceiling of 5% tender premium. Consequently, 578 tenders valuing ₹389.15 crore were irregularly awarded at premiums exceeding the limit.

b. Participation of blacklisted/ineligible bidders: The application lacked controls to disable logins of blacklisted suppliers, leading to contracts worth ₹2.43 crore being awarded to blacklisted firms. It also allowed ineligible contractors to bid for high-value works beyond their registration class.

11. Uttar Pradesh

Digitisation through GePNIC enabled online tender publication, bid submission and electronic storage of tender documents across a large number of procuring entities. However, certain gaps were observed by audit which are listed below:

i. Manual intervention at multiple stages of the tender lifecycle, including technical evaluation, bid capacity assessment, EMD management and award of contract, diluted the effectiveness of end-to-end electronic processing.

ii. The system provides for disclosure of tender stages, bid details and outcomes on a public portal. Audit observed that non-uploading of Awards of Contract, incorrect tender status updates and offline processing of bids resulted in incomplete visibility of procurement outcomes and weakened the audit trail.

iii. Electronic tendering reduced initial transaction time and facilitated wider bidder participation. Nevertheless, large volumes of tenders remained pending at intermediate stages, contracts were executed with significant delays, and system functionalities such as online technical evaluation were not implemented, limiting efficiency gains.

iv. Institutional mechanisms envisaged under the Project Proposal Document — such as the Core Committee, Process Advisory Committee and Project Monitoring Unit — were not operationalised. As a result, post-implementation monitoring, system enhancement and user adoption were not adequately driven.

v. Audit identified systemic control weaknesses in user access management, mapping of business rules, validation of critical dates, input controls during bidder registration and tender cancellation, and management of EMD and performance securities. These weaknesses increased reliance on manual controls and administrative discretion.

vi. Absence of robust audit trails, inconsistencies in bid decryption timestamps, discrepancies in generation of comparative financial statements and related risk of backend access raised concerns regarding data integrity and non-repudiation, notwithstanding certification of the system by MeitY.

vii. Analysis of large-scale transactional data indicated repeated participation of bidders using common IP addresses, mobile numbers, email IDs and other credentials, including instances where bidder and departmental user IP addresses overlapped. Inadequate analytical and preventive controls within the system limited the ability to detect and deter collusive bidding and cartelisation.

Some illustrations:

a. Erroneous financial calculations: The system's automated comparative financial charts erroneously calculated the final bid values in percentage-rate tenders, producing flawed L1 evaluations. Moreover, comparative charts were generated on different dates and subsequently removed from the portal, indicating backend data tampering.

b. Bid decryption chronology: Bids were recorded in the database as decrypted *before* they were even submitted by the bidders. Additionally, bids were decrypted while the tender status was still locked at 'to_be_opened', proving unauthorized backend access.

12. West Bengal

West Bengal mandated eProcurement for tenders of ₹50 lakh and above in 2012, progressively reducing the threshold to ₹1 lakh by 2022. The portal has handled nearly 9.76 lakh tenders worth ₹5.23 lakh crore, with wide departmental adoption. However, certain gaps were observed by audit which are listed below:

i. Full coverage has not been achieved — Parliamentary Affairs and Law Departments, 18 PSUs and 68 autonomous bodies had not registered or used the portal as of March 2023. End-to-end digitisation was also not achieved as bid evaluation and contract award were conducted entirely outside the system.

ii. Evaluation and award of tenders were conducted outside the system, with only scanned summaries uploaded later. Functionality for negotiations with L1 bidders was absent, forcing offline handling and leaving no audit trail. PWD Divisions circumvented mandatory thresholds by splitting works into smaller tenders floated offline. Delays of up to 1,769 days were observed in uploading Award of Contract data, leading to delayed EMD refunds and incorrect MIS reports.

iii. Efficiency goals were undermined on multiple fronts: Unsuccessful bidders waited beyond mandated timelines for EMD refunds, while successful bidder deposits were delayed by banks. Tie-breaks and negotiations were handled outside the system, slowing processing. Contracts in 1,291 cases were awarded at values exceeding the L1 bid due to manual interventions.

iv. Project governance was weak. No MoU or SLA existed between the Government of West Bengal and NIC, exposing the State to risks of unclear accountability. The State Level Core Committee (SLCC) was inactive from 2019 to 2023, reducing oversight of portal implementation and monitoring. Change management was poorly documented, with software version changes lacking proper records and risking accountability lapses.

v. Key control failures were observed across multiple dimensions. Non-Tender Inviting Authorities (TIAs) such as Assistant Engineers and Superintending Engineers irregularly published tenders using the IDs of Executive Engineers. Expired and irregular DSCs issued to ineligible staff compromised authority and non-repudiation. Duplicate or invalid PANs were found in 12,201 instances, with multiple bidder IDs linked to the same mobile number or email address, and minors registered as bidders. The system did not enforce minimum bid submission periods, the two-bid process for tenders above ₹10 lakh or BoQ auto-computation.

vi. Null hash values for encrypted BoQs were found in three per cent of cases during 2018-23, undermining confidence in bid integrity. Broken chronology in timestamps and gaps in sequence IDs suggested possible backend tampering. Non-renewal of the MoU with ICICI Bank led to delays in EMD deposits and refunds and loss of penal interest.

vii. Audit analysis identified multiple bidders in the same tender using the same PAN, mobile number or email ID, reducing effective competition. Tenders with fewer than three unique bidders were processed despite policy requiring re-tendering in such cases, vitiating open competition.

Some illustrations:

a. Null hash values and database tampering: The cryptographic hash values for 1,85,928 uploaded BOQ documents were recorded as 'null' in the database. Combined with massive missing sequential IDs in the gep_bids table (over 2.56 lakh cases), this indicates a catastrophic failure of cryptographic non-repudiation and points to direct backend manipulation of bid data.

b. Opening financial bids without technical decryption: The system irregularly permitted bid openers to decrypt and evaluate financial bids without any corresponding system record that the technical bids for those specific bidders had ever been decrypted or qualified.

V. Recommendations

The following structured recommendations, organised by time-horizon, are addressed to State Governments and the Ministry of Finance/MeitY as appropriate. We consider that implementation would be driven by a designated nodal authority with defined accountability.

Short-Term Recommendations (0 – 6 Months)

State Governments to immediately:

i. Strengthen access and identity controls by validating all bidder/user data (PAN, mobile, email, DSC), reviewing all user accounts, disabling inactive and unauthorised IDs, and enforcing maker-checker segregation of duties across the tender lifecycle.

ii. Issue formal directives mandating end-to-end online procurement for all eligible procurements, explicitly prohibiting parallel offline processes, and ensuring strict adherence to system-generated tender timelines.

iii. Improve transparency of procurement outcomes by ensuring timely updating of all tender stages and making mandatory the uploading of awards of contract and supporting evaluation documents within a prescribed period.

iv. Embed key procurement rules into the system as a priority, including minimum bid periods, prescribed bid structures, automated BoQ computations, and system-generated comparative statements.

v. Strengthen financial and audit controls through integrated online EMD payment and refund mechanisms, and define audit log retention and archival requirements.

vi. Deploy automated alerts and data analytics to detect duplicate credentials, shared IP/PAN/email IDs, corrigenda or extensions, and abnormal bidding patterns indicative of collusion.

vii. Formalise governance mechanisms by executing MoU/SLAs with NIC and other service providers, and activating all oversight committees with defined quorum and meeting schedules.

Medium-Term Recommendations (6 Months – 2 Years)

State Governments to:

i. Implement end-to-end system-based tender processing including automated computation of bid timelines and EMD, online technical and financial bid evaluation, automated bid-capacity computation, system-based negotiation and contract award.

ii. Strengthen application-level validations across the entire tender lifecycle: bidder registration, DSC enforcement, critical dates, modifications, corrigenda issuance, bid opening, cancellation reasons and EMD workflows.

iii. Implement structured MIS, dashboards and exception reporting covering age analysis of tenders, pendency at intermediate stages, AoC delays, pending EMD refunds, and bidder credential anomalies.

iv. Deploy advanced analytics for competition and risk monitoring to flag common IP addresses, PANs, mobile numbers, abnormal bidding patterns and potential collusion indicators in real time.

v. Institutionalise periodic internal and IS Audits of the e-Procurement system to assess control effectiveness, ensure STQC compliance, and maintain updated security certifications.

vi. Operationalise a fully staffed Project Monitoring Unit and institutionalise capacity-building measures including regular training for departmental users and vendor awareness programmes.

vii. Formalise change-management processes to govern system enhancements, configuration changes and procurement rule updates.

Long-Term Recommendations (2 – 3 Years)

State Governments to:

i. Achieve end-to-end digitisation of the procurement lifecycle by implementing all missing modules, indent management, contract management and catalogue management and mandating system-generated Letters of Award with complete audit trails.

ii. Establish a formal State-level e-Procurement Governance Authority with clearly defined ownership, accountability, escalation mechanisms and enforcement powers, incorporating Core Committee, PAC and PMU functions.

iii. Redesign and periodically upgrade the system architecture to embed procurement rules, non-repudiation controls, comprehensive audit trails and security features aligned with evolving procurement practices.

iv. Implement advanced audit-trail, log-analytics and secure archival solutions to strengthen transparency, forensic readiness and long-term data integrity.

v. Integrate e-Procurement with related platforms including PFMS, GeM, IFMS/IFMIS, contract management systems and vendor performance databases to create a seamless, end-to-end public procurement ecosystem.

vi. Institutionalise periodic independent system, IS and security audits, including certifications, performance reviews and continuous improvement mechanisms.

vii. Build in-house IT and audit capabilities to reduce over-dependence on service providers, ensuring the State retains effective oversight and control over the e-Procurement platform, including source code access.

viii. Leverage emerging technologies including Artificial Intelligence for anomaly detection, blockchain for tamper-proof audit trails, and Robotic Process Automation for repetitive procurement workflows.

* * * * * *

Annexure-I: Status of IS Audit Reports on e-Procurement Systems in the States

S. No	Name of the State	Status of IS Audit
1	Andhra Pradesh	Management Letter issued to Government
2	Assam	Tabled in State Legislative Assembly
3	GNCT of Delhi	Approved and yet to tabled in State Legislative Assembly
4	Haryana	Audit is completed and in the process of Approval
5	Himachal Pradesh	Approved and yet to tabled in State Legislative Assembly
6	Jharkhand	Audit is completed and in the process of Approval
7	Odisha	Tabled in State Legislative Assembly
8	Punjab	Tabled in State Legislative Assembly
9	Tamil Nadu	Tabled in State Legislative Assembly
10	Telangana	Management Letter issued to Government
11	Uttar Pradesh	Approved and yet to tabled in State Legislative Assembly
12	West Bengal	Approved and yet to tabled in State Legislative Assembly

Glossary of Abbreviations

Abbreviation	Full Form
AoC	Award of Contract
BoQ	Bill of Quantities
CAG	Comptroller and Auditor General of India
CAATs	Computer Assisted Audit Techniques
CVC	Central Vigilance Commission
DR	Disaster Recovery
DSC	Digital Signature Certificate
EMD	Earnest Money Deposit
GeM	Government e-Marketplace
GePNIC	Government e-Procurement System developed by NIC
GFR	General Financial Rules
HLSD/LLSD	High Level / Low Level System Design
IFMS/IFMIS	Integrated Financial Management System
IP	Internet Protocol
IS Audit	Information Systems Audit
L1	Lowest Responsive Bidder
MIS	Management Information System
MoU	Memorandum of Understanding
MSA	Master Service Agreement
NeGP	National e-Governance Plan
NIC	National Informatics Centre
NIT	Notice Inviting Tender
PAC	Process Advisory Committee
PFMS	Public Financial Management System
PKI	Public Key Infrastructure
PMU	Project Monitoring Unit
SLA	Service Level Agreement
SLCC	State Level Core Committee
SSCA	Subject Specific Compliance Audit
STQC	Standardisation Testing and Quality Certification
TIA	Tender Inviting Authority

WAMIS	Works Accounts Management Information System